9. Security, Identity and Compliance

AWS Certificate Manager (ACM)

O AWS Certificate Manager (ACM) facilita o provisionamento, o gerenciamento, a implantação e a renovação de certificados SSL/TLS na plataforma da AWS.

O AWS Certificate Manager é um serviço que permite provisionar, gerenciar e implantar facilmente certificados Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para uso com os serviços da AWS e os recursos internos conectados.

Os certificados SSL/TLS são usados para proteger comunicações de rede e estabelecer a identidade de sites na Internet e de recursos em redes privadas. O AWS Certificate Manager elimina processos manuais demorados como compra, upload e renovação de certificados SSL/TLS.

Com o AWS Certificate Manager, você pode solicitar rapidamente um certificado, implantá-lo em recursos da AWS integrados ao ACM, como Elastic Load Balancers, distribuições do Amazon CloudFront e APIs no Amazon API Gateway, e deixar que o AWS Certificate Manager administre as renovações desses certificados.

O serviço também permite criar certificados privados para recursos internos e centralizar o gerenciamento do ciclo de vida dos certificados.

Recursos

Gerenciamento Seguro de Chaves: O AWS Certificate Manager foi desenvolvido para proteger e gerenciar chaves privadas usadas com certificados SSL/TLS. As melhores práticas de criptografia forte e gerenciamento de chave são usadas ao proteger e armazenar chaves privadas.

Autoridade de Certificados Privada: A autoridade de certificação (AC) privada do AWS Certificate Manager (ACM) é um serviço gerenciado de AC privada que ajuda a gerenciar com facilidade e segurança o ciclo de vida de certificados privados. A AC privada do ACM disponibiliza um serviço de AC privada altamente disponível, sem o investimento adiantado e os custos de manutenção contínua da operação de uma AC privada própria ou de uma hierarquia privada de AC.

Importe Certificado de Terceiros: O AWS Certificate Manager facilita importar certificados SSL/TLS emitidos por Autoridades de certificação (CAs) de terceiros e implantá-los usando Elastic Load Balancers, distribuições do Amazon CloudFront e APIs no Amazon API Gateway. É possível monitorar a data de expiração de um certificado importado e importar um substituto quando o certificado atual estiver prestes a expirar. Como alternativa, você pode solicitar um certificado gratuito por meio do AWS Certificate Manager e permitir que a AWS gerencie renovações para você. A importação de certificados é gratuita.

Adicionar Nomes de Domínio: Digite o nome de domínio totalmente qualificado do site que você deseja proteger com um certificado SSL/TLS (por exemplo, www.example.com). Use um asterisco (*) para solicitar um certificado curinga para proteger vários sites no mesmo domínio. Por exemplo: *.example.com protege www.example.com, site.example.com e images.example.com. Antes de emitir seu certificado, precisamos validar que você possui ou controla os domínios para os quais está solicitando o certificado. O ACM pode validar a propriedade usando o DNS ou enviando um e-mail para os endereços de contato do proprietário do domínio

Definição de Preço

Os certificados públicos e privados provisionados pelo AWS Certificate Manager para uso com serviços integrados ao ACM são gratuitos. Você paga apenas pelos recursos da AWS que criar para executar seu aplicativo.

O preço da autoridade de certificados (AC) privada do ACM é definido por duas dimensões. Você paga uma taxa mensal pela operação de cada AC privada até que ela seja excluída e paga mensalmente pelos certificados privados emitidos.

AWS Directory Service

O Active Directory é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes Windows, presentes no active directory.

O AWS Directory Service fornece várias maneiras de usar o Microsoft Active Directory (AD) com outros serviços da AWS.

Os diretórios armazenam informações sobre usuários, grupos e dispositivos, e os administradores utilizam eles para gerenciar o acesso a informações e recursos.

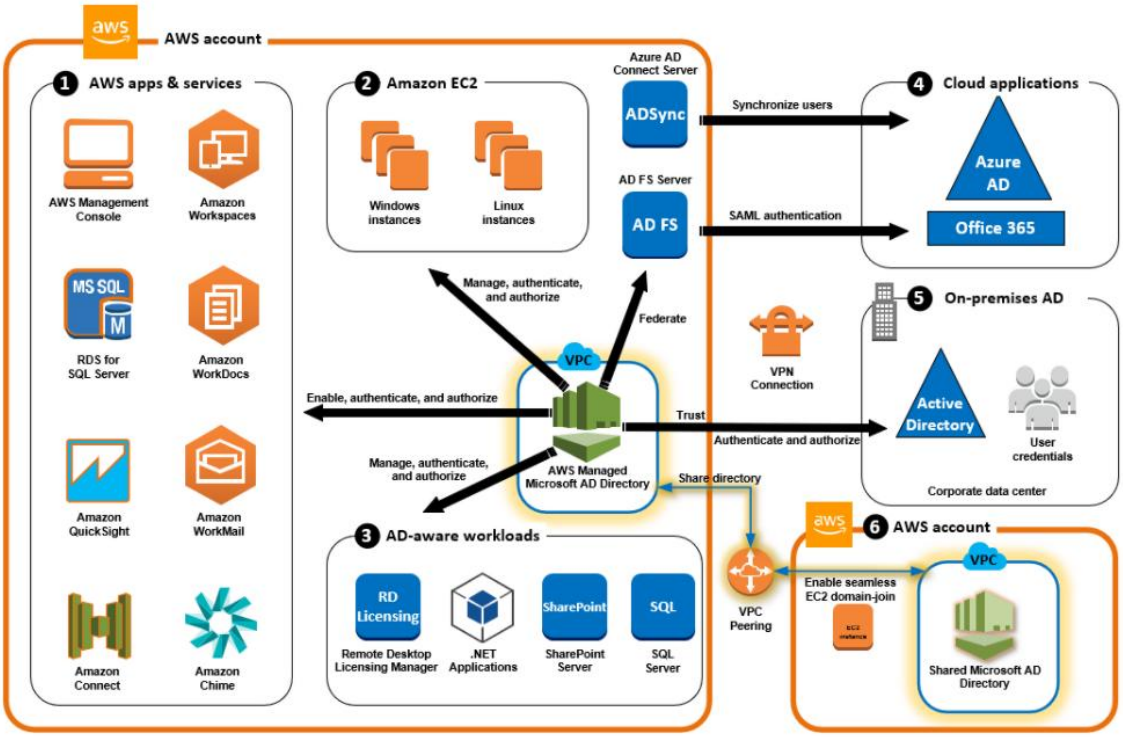
AWS Directory Service fornece várias opções de diretórios para os clientes que desejam usar aplicativos existentes habilitados para Microsoft AD ou Lightweight Directory Access Protocol (LDAP) na nuvem.

Ele também oferece essas mesmas opções para os desenvolvedores que precisam de um diretório para gerenciar usuários, grupos, dispositivos e acesso.

Com o AWS Managed Microsoft AD, você pode ingressar facilmente as instâncias do Amazon EC2 e do Amazon RDS for SQL Server em um domínio e usar os serviços do AWS End User Computing (EUC), como o Amazon WorkSpaces, com os usuários e grupos do AD.

Com AWS Microsoft AD gerenciado, você pode compartilhar um único diretório para vários casos de uso. Por exemplo, você pode compartilhar um diretório para autenticar e autorizar o acesso para aplicativos .NET, Amazon RDS para SQL Server por Autenticação Habilitado e Amazon Chime para mensagens e videoconferência.

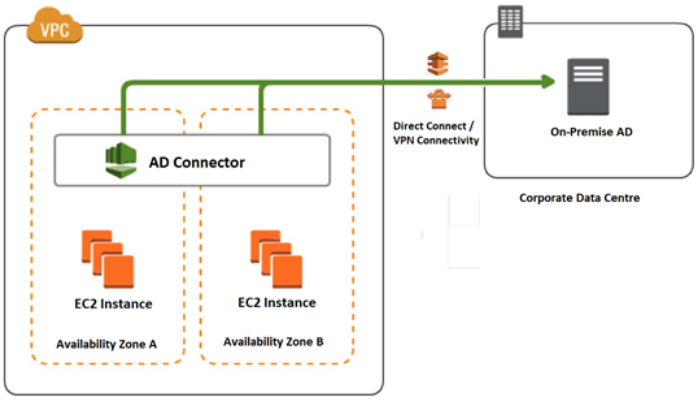
O diagrama a seguir mostra alguns casos de uso para o AWS Diretório do Microsoft AD gerenciado pela. Isso inclui a capacidade de conceder aos usuários acesso aos aplicativos de nuvem externos e permitir que os usuários do AD no local gerenciem e tenham acesso aos recursos na Nuvem AWS.



AD Connector

Uma empresa de TI global tem uma conectividade híbrida para seus servidores de aplicativos implantados em um data center local e infraestrutura em nuvem AWS. Os desenvolvedores projetaram um novo aplicativo que será implantado em ambos os locais e espera ser acessado por 4.000 usuários em todo o mundo. A equipe de segurança do cliente exige que as mesmas políticas de segurança sejam aplicadas aos usuários ao acessar novos aplicativos de

servidores locais ou da nuvem AWS. Um cliente já implantou um Active Directory no local com toda a conformidade de segurança. O chefe de TI o informou sobre as restrições de orçamento e nenhum custo adicional deve ser incorrido para uma nova solução. Qual das opções a seguir pode ser usada para projetar serviços AD para novos aplicativos? **R: Use AD Connector.**



Usando um conector AD, os clientes podem usar o AD existente implantado em servidores locais. Para isso, nenhuma implantação adicional é necessária, apenas sobre a conectividade VPN / DX existente. Todas as solicitações podem ser encaminhadas para o AD local. Com isso, as mesmas políticas de segurança podem ser aplicadas tanto para o local quanto para usuários que acessam da nuvem. Com o AWS Managed Active Directory Service ou a implantação de AD na instância do Amazon EC2, haverá um custo adicional para a implantação de AD separado na nuvem AWS. O AD simples não encaminha solicitações para o AD local. Portanto, as políticas de segurança não podem ser as mesmas.

➢ Pontos de Atenção

1. Com seu próprio Active Directory, sua empresa autentica usuários para diferentes aplicativos. Você recebeu a tarefa de consolidar e migrar serviços para a nuvem e usar as mesmas credenciais, se possível. O que você recomendaria? **R: Use AWS Directory Service that allows users to sign in with their existing corporate credentials.** *AWS Directory Service enables your end-users to use their existing corporate credentials while accessing AWS applications. Once you've been able to consolidate services to AWS, you won't have to create new credentials. Instead, you'll be able to allow the users to use their existing username/password.*

2. Você tem uma pequena empresa, executando no sistema operacional Windows, que aproveita recursos de nuvem como AWS Workspaces e AWS Workmail. Você deseja uma solução totalmente gerenciada para definir políticas e fornecer gerenciamento de usuários. Qual do AWS Directory Service mínimo necessário você recomendaria? **R: Simple AD for limited functionality and compatibility with desired applications.** *Simple AD for limited functionality and compatibility with desired applications is the correct answer. Simple AD is a Microsoft Active Directory–compatible directory from AWS Directory Service. You can use Simple AD as a standalone directory in the cloud to support Windows workloads that need basic AD features or compatible AWS applications. It can also be used to support Linux workloads that need LDAP service.*

Amazon GuardDuty

O Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos não autorizados para proteger suas contas, cargas de trabalho e dados da AWS armazenados no Amazon S3.

Com a nuvem, a coleta e a agregação de contas e atividades de rede é simplificada, mas pode ser demorado para as equipes de segurança analisarem continuamente os dados de logs de eventos em busca de possíveis ameaças.

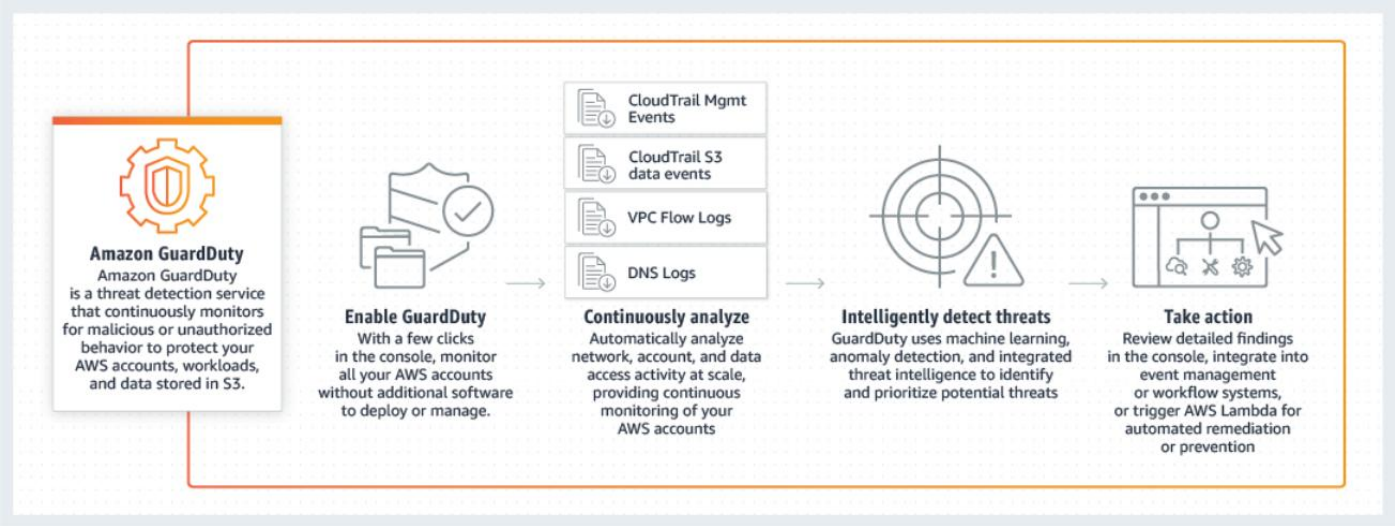
Com o GuardDuty, agora você tem uma opção inteligente e econômica para a detecção contínua de ameaças na AWS.

O serviço usa machine learning, detecção de anomalias e inteligência integrada contra ameaças para identificar e priorizar possíveis ameaças.

O GuardDuty analisa dezenas de bilhões de eventos em várias fontes de dados da AWS, como logs de eventos do AWS CloudTrail, Amazon VPC Flow Logs e logs de DNS.

Com alguns cliques no Console de Gerenciamento da AWS, é possível habilitar o GuardDuty sem nenhum software ou hardware para implantar ou manter.

Com integração ao Amazon CloudWatch Events, os alertas do GuardDuty são práticos, fáceis de agregar entre várias contas e simples de implantar em sistemas existentes de gerenciamento de eventos e fluxos de trabalho.



AWS Identity and Access Management (IAM)

O AWS IAM – Identity and Access Management permite gerenciar com segurança o acesso aos serviços e recursos da AWS. Usando o IAM, é possível criar e gerenciar usuários e grupos da AWS e usar permissões para conceder e negar acesso a recursos da AWS, sendo totalmente gratuito.

Controle de **acesso minucioso** para seus recursos da AWS: O IAM permite que os usuários controlem o acesso às APIs de serviço e a recursos específicos da AWS. O IAM também permite que seja adicionado **condições específicas**, como hora certa para controlar como um usuário pode usar a AWS, seu endereço IP de origem, se estão usando SSL ou se fizeram a autenticação com um dispositivo de autenticação multifator.

Identidades do IAM

Usuário Raiz: Ao criar uma conta da AWS, você começa com uma única identidade de login que tem acesso total a todos os serviços e recursos da AWS na conta. Essa identidade é chamada de usuário raiz da conta e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. A própria AWS recomenda não usar o usuário raiz para as tarefas diárias nem mesmo para as tarefas administrativas

Políticas do IAM

Uma política é um objeto na AWS que, quando associado a uma identidade ou a um recurso, define suas permissões

Função do IAM

Uma função do IAM é uma identidade do IAM que se pode criar na conta com permissões especificas. Você pode usar funções para delegar acesso a usuários, aplicativos ou serviços que normalmente não tem acesso aos seus recursos da AWS. Em um breve resumo, uma Função é um conjunto das políticas, ou seja, várias políticas formam uma Função

Usuário do IAM

O usuário do IAM representa a pessoa ou o serviço que usa o usuário do IAM para interagir com a AWS. Seu uso principal é oferecer às pessoas a capacidade de entrar no Console de gerenciamento da AWS ou solicitações programáticas aos servidores da AWS, usando a API ou a CLI

Concede-se a ele permissões tornando-o um membro de um grupo com **políticas de permissão** apropriadas anexadas (recomendadas) ou anexando diretamente políticas ao usuário

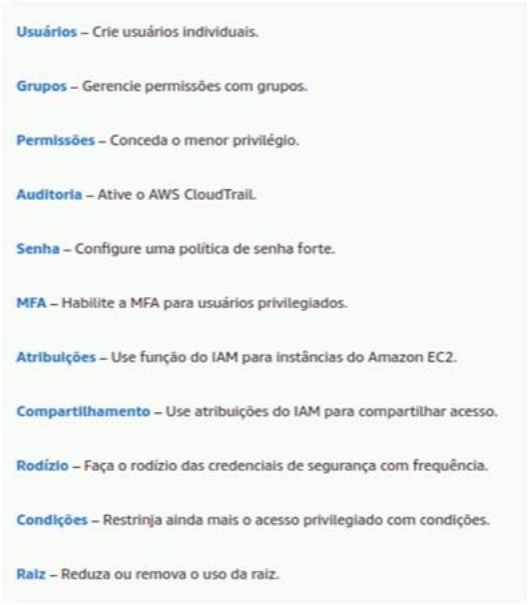
Grupos do IAM

Um grupo do IAM é um conjunto de usuários do IAM. Pode-se usar grupos para especificar permissões para um conjunto de usuários, o que pode facilitar o gerenciamento dessas permissões para esses usuários. Lembrando que é possível setar as permissões para cada usuário individualmente

Credenciais Temporárias

O IAM também permite que se conceda aos usuários credencias temporárias de segurança com uma expiração definida para dar acesso aos seus recursos da AWS

Melhores Práticas do IAM



Quando criar um usuário do IAM?

Quando uma pessoa precisa de acesso para acessar os recursos da AWS

Quando criar uma função do IAM?

Quando um serviço, aplicativo ou recurso precisa acessar os recursos da AWS (inclusive outros serviços da AWS)

Ou quando usuários da empresa estão autenticados na rede corporativa e desejam utilizar a AWS sem a necessidade de realizar login novamente

Quando criar uma política personalizada?

Quando se não há uma política pronta com os acessos e recursos desejados para atribuir a um ou mais usuário, grupo ou função da conta

Sobre a federação de identidades da Web

Imagine que você esteja criando um aplicativo móvel que acesse recursos da AWS, como um jogo que seja executado em um dispositivo móvel e armazene informações de pontuação e dos jogadores usando o Amazon S3 e o DynamoDB.

Ao elaborar um aplicativo como esse, você fará solicitações para os serviços da AWS que devem ser assinados com uma chave de acesso da AWS. No entanto, é altamente recomendável que você não incorpore nem distribua credenciais de longo prazo da AWS com aplicativos dos quais um usuário faça download para um dispositivo, mesmo em um armazenamento criptografado. Em vez disso, crie seu aplicativo para que ele solicite credenciais de segurança temporárias da AWS dinamicamente quando necessário usando a *federação de identidades da web*. As credenciais temporárias fornecidas são mapeadas para uma função da AWS que têm apenas as permissões necessárias para executar as tarefas necessárias ao aplicativo móvel.

Com a federação de identidades da web, você não precisa criar código de login personalizado nem gerenciar suas próprias identidades de usuários. Em vez disso, os usuários de seu aplicativo podem fazer login usando um provedor de identidades externo (IdP) conhecido, como Login with Amazon, Facebook, Google ou qualquer outro IdP compatível com OpenID Connect (OIDC). Eles podem receber um token de autenticação e, em seguida, trocar esse token por credenciais de segurança temporárias no AWS que são mapeadas para uma função do IAM com

permissões para usar os recursos na sua conta do AWS. O uso de um IdP ajuda você a manter sua conta da AWS segura, pois você não precisa incorporar e distribuir credenciais de segurança de longo prazo com seu aplicativo.

Para a maioria dos cenários, recomendamos que você use Amazon Cognito porque ele atua como um agente de identidades e faz boa parte da federação trabalhar para você. Para obter detalhes, consulte a seção a seguir, Usar o Amazon Cognito para aplicações móveis.

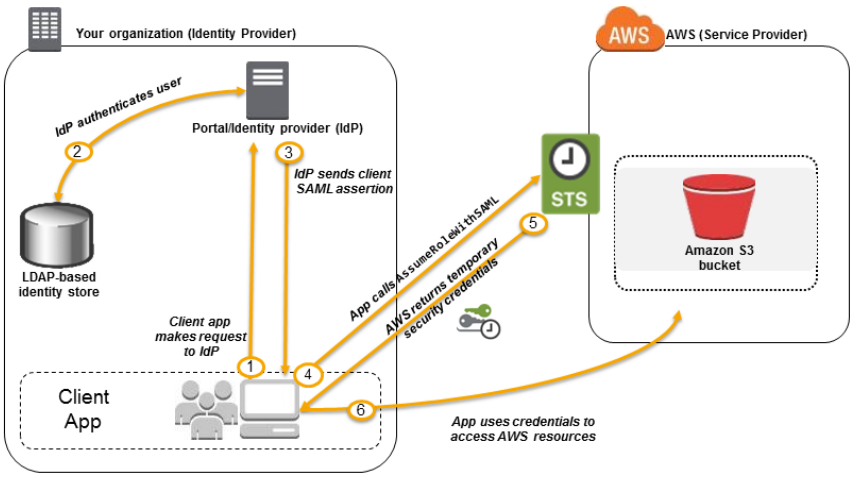
Se você não usar o Amazon Cognito, deverá elaborar um código que interaja com um IdP da web, como Facebook, e, em seguida, chamar a API AssumeRoleWithWebIdentity para trocar o token de autenticação obtido desses IdPs por credenciais de segurança temporárias do AWS. Se você já usou essa abordagem para aplicativos existentes, poderá continuar a usá-lo.

Sobre a federação baseada em SAML 2.0

A AWS dá suporte à federação de identidades com o SAML 2.0 (Security Assertion Markup Language 2.0), um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso habilita o logon único (SSO) federado, para que usuários possam fazer login no AWS Management Console ou chamar as operações de API da AWS sem precisar criar um usuário do IAM para todos em sua organização. Ao usar o SAML, simplifique o processo de configuração da federação com a AWS, pois poderá usar o serviço do IdP, em vez de gravar o código de proxy de identidade personalizado.

Usar a federação baseada em SAML para acesso da API à AWS

Imagine que você deseja fornecer uma maneira para os funcionários copiarem dados de seus computadores para uma pasta de backup. Crie um aplicativo que possa ser executado pelos usuários em seus computadores. No back-end, o aplicativo lê e grava objetos em um bucket do S3. Os usuários não têm acesso direto à AWS. Em vez disso, o processo seguinte é usado:



Cross-account IAM roles

No momento, você entrou em contato com um parceiro da AWS para realizar uma auditoria em sua conta da AWS. Você precisa se certificar de que o parceiro pode realizar uma auditoria em seus recursos. Qual das seguintes etapas você idealmente executaria? **R: Create a cross account IAM Role.**

As funções de IAM entre contas permitem que os clientes concedam com segurança acesso aos recursos da AWS em suas contas a terceiros, como um parceiro APN, enquanto retêm a capacidade de controlar e auditar quem está acessando sua conta da AWS. As funções de contas cruzadas reduzem a quantidade de informações confidenciais que os parceiros APN precisam armazenar para seus clientes, para que possam se concentrar em seus produtos em vez de gerenciar as chaves.

O acesso entre contas é mais seguro porque, Uma analogia básica da diferença é entregar a alguém um crachá de acesso (que pode ser usado por qualquer pessoa) em vez de entregar a alguém um crachá de acesso que requer as impressões digitais dessa pessoa para usar com sucesso.

Usar um usuário IAM para controlar o acesso de terceiros envolve a entrega de uma chave de acesso / chave secreta - esse é o simples "crachá de acesso".

Usar AssumeRole para controlar o acesso de terceiros usa as mesmas informações mais um token de segurança. Para assumir uma função, sua conta da AWS deve ser confiável para a função. A relação de confiança é definida na política de confiança da função quando a função é criada. Este é o "crachá de acesso com validação de impressão digital."

(Além disso, para aumentar a segurança, a chave de acesso / chave secreta para AssumeRole pode ser credenciais temporárias que expiram após um período de tempo específico.)

Qualquer pessoa pode usar as chaves IAM - elas são apenas um par de chaves. Qualquer pessoa pode pegá-los e usá-los mais tarde, e você não será identificado pela parte de confiança para quem foram dados. Para usar o AssumeRole, você deve primeiro ser autenticado como a entidade confiável e, no caso de credenciais temporárias, usá-las enquanto não expiraram. Esses recursos extras de segurança são o que o torna mais seguro.

Typically, you use AssumeRole for cross-account access.

➢ Pontos de Atenção

1. Você tem um novo membro em sua organização. Você provisionou um usuário IAM para o novo funcionário na AWS, no entanto, o usuário não pode realizar nenhuma ação. Qual poderia ser o motivo disso? **R: Os usuários IAM são criados por padrão, sem permissões**

2. Você é o arquiteto de soluções da conta AWS da sua empresa com aproximadamente 300 usuários IAM. Eles têm uma nova política da empresa que mudará o acesso de 100 dos usuários IAM para ter um tipo específico de acesso aos buckets do Amazon S3. O que você fará para evitar a tarefa demorada de aplicar a política ao usuário individual? R: Crie um novo grupo IAM e, em seguida, adicione os usuários que requerem acesso ao intervalo S3. Depois, aplique a política ao grupo IAM.

3. Um de seus clientes deseja aproveitar o Amazon S3 e o Amazon Glacier como parte de sua infraestrutura de backup e arquivamento. Eles criaram um novo bucket S3 chamado “clubecloudbucket”. Para oferecer suporte a essa integração entre a AWS e sua rede local, eles decidiram usar um software de terceiros. Qual abordagem limitará o acesso do software de terceiros apenas ao bucket do Amazon S3 e não a outros recursos da AWS? R: No IAM, configure uma política de usuário personalizada para o software de terceiros que é limitada à API do Amazon S3 no bucket "clubecloudbucket".

4. Você tem instâncias EC2 em execução em seu VPC. Você tem instâncias do UAT e EC2 de produção em execução. Você deseja garantir que os funcionários responsáveis pelas instâncias do UAT não tenham acesso para trabalhar nas instâncias de produção para minimizar os riscos de segurança. Qual das opções a seguir seria a melhor maneira de conseguir isso? R: Defina as tags nos servidores UAT e de produção e adicione uma condição à política IAM que permite o acesso a tags específicas.

5. You deployed a web application to an EC2 instance that adds a variety of photo effects to a picture uploaded by the users. The application will put the generated photos to an S3 bucket by sending PUT requests to the S3 API. What is the best option for this scenario considering that you need to have API credentials to be able to send a request to the S3 API? R: Create a role in IAM. Afterwards, assign this role to a new EC2 instance.

6. You recently created a brand new IAM User with a default setting using AWS CLI. This is intended to be used to send API requests to your S3, DynamoDB, Lambda, and other AWS resources of your cloud infrastructure. Which of the following must be done to allow the user to make API calls to your AWS resources? R: Create a set of Access Keys for the user and attach the necessary permissions.

7. An AWS account has an ID of 201920192033. Which of the following URLs would you provide to the IAM user to be able to access the AWS Console? R: https://201920192033.signin.aws.amazon.com/console

8. O login de terceiros (Federação) foi implementado em seu aplicativo da web para permitir que os usuários que precisem acessar os recursos da AWS. Os usuários têm feito login com sucesso usando o Google, Facebook e outras credenciais de terceiros. De repente, seu acesso a alguns recursos da AWS foi restringido. Qual é a causa mais provável do uso restrito de recursos da AWS? R: IAM policies for resources were changed, thereby restricting access to AWS resources.

AWS Security Token Service (STS)

AWS Security Token Service (AWS STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users).

Endpoints

By default, AWS Security Token Service (AWS STS) is available as a global service, and all AWS STS requests go to a single endpoint at https://sts.amazonaws.com. Global requests map to the US East (N. Virginia) Region. AWS recommends using Regional AWS STS endpoints instead of the global endpoint to reduce latency, build in redundancy, and increase session token validity.

Recording API requests

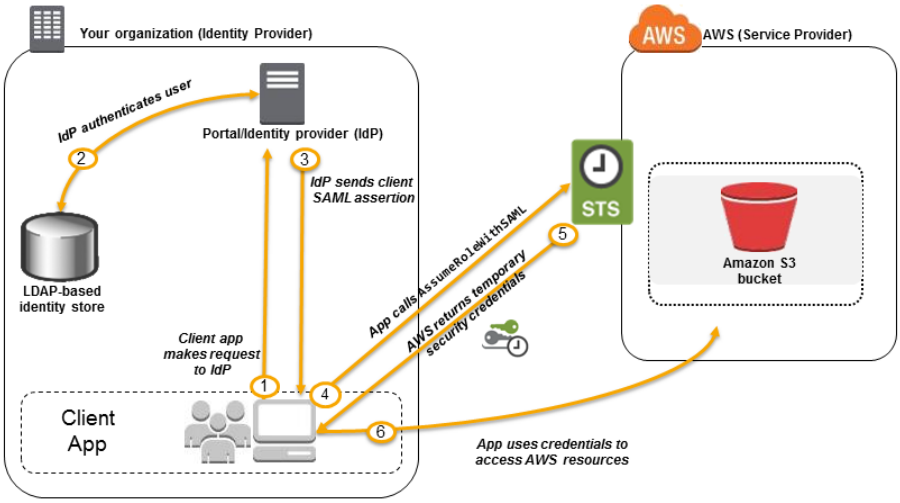
AWS STS supports AWS CloudTrail, which is a service that records AWS calls for your AWS account and delivers log files to an Amazon S3 bucket. By using information collected by CloudTrail, you can determine what requests were successfully made to AWS STS, who made the request, when it was made, and so on.

Features

- STS enables you to request temporary, limited-privilege credentials.
- STS enables users to assume role.
- By default, AWS STS is available as a global service.

Using SAML-Based Federation for API Access to AWS

Imagine that in your organization, you want to provide a way for users to copy data from their computers to a backup folder. You build an application that users can run on their computers. On the back end, the application reads and writes objects in an S3 bucket. Users don't have direct access to AWS. Instead, the following process is used:



➢ Pontos de Atenção

1. Your organization AWS Setup has an AWS S3 bucket which stores confidential documents which can be only downloaded by users authenticated and authorized via your application. You do not want to create IAM users for each of these users and as a best practice you have decided to generate AWS STS Federated User temporary credentials each time when a download request is made and then use the credentials to generate presigned URL and redirect user for download. However, when user is trying to access the presigned URL, they are getting Access Denied Error. What could be the reason? R: IAM User used to generate Federated User credentials does not have access on S3 bucket.

2. Your organization has an AWS setup and planning to build Single Sign On for users to authenticate with on-premise Microsoft Active Directory Federation Services (ADFS) and let users login to AWS console using AWS STS Enterprise Identity Federation. Which of the following API should be used with AWS STS service after you authenticate with your on-premise? R: AssumeRoleWithSAML

Amazon Inspector

Serviço automatizado de avaliação de segurança que ajuda a melhorar a segurança e a conformidade de aplicativos implantados na AWS

O Amazon Inspector é um serviço de avaliação de segurança automático que ajuda a melhorar a segurança e a conformidade dos aplicativos implantados na AWS.

O Amazon Inspector avalia automaticamente aplicativos em busca de exposições, vulnerabilidades ou discrepâncias em relação às melhores práticas.

Após realizar uma avaliação, o Amazon Inspector produz uma lista detalhada de descobertas de segurança priorizadas de acordo com o nível de severidade.

Essas descobertas podem ser revisadas diretamente ou como parte de relatórios de avaliação detalhados, disponibilizados no console ou pelas APIs do Amazon Inspector.

As avaliações de segurança do Amazon Inspector ajudam a verificar a existência de acessibilidade de rede não intencional em instâncias do Amazon EC2 e de vulnerabilidades nessas instâncias do EC2.

As avaliações do Amazon Inspector são fornecidas como pacotes de regras predefinidas, associadas a melhores práticas de segurança e definições de vulnerabilidades comuns.

Os exemplos de regras integradas incluem a verificação de acesso da Internet a instâncias do EC2, habilitação de login de raiz remoto ou instalação de versões de software vulneráveis.

Essas regras são atualizadas regularmente pelos pesquisadores de segurança da AWS.

Definição de Preço

O Amazon Inspector é um serviço de avaliação de segurança para instâncias do Amazon EC2 e para os aplicativos executados nessas instâncias.

A definição de preço é baseada em duas dimensões: o número de instâncias do EC2 incluídas em cada avaliação e os tipos de pacotes de regras selecionados.

Uma avaliação do Inspector pode ter qualquer combinação dos dois tipos de pacote de regras: pacotes de regras de avaliação de host e/ou pacotes de regras de acessibilidade de rede.

Os pacotes de avaliação de host incluem Common Vulnerabilities and Exposures (CVEs – Vulnerabilidades e exposições comuns), testes comparativos do Center for Internet Security (CIS), melhores práticas de segurança e análise de comportamento em tempo de execução.

Se as avaliações incluírem pacotes de regras de host e de acessibilidade de rede, os pacotes serão cobrados separadamente.

AWS Key Management Service (AWS KMS)

O AWS Key Management Service (KMS) facilita a criação e o gerenciamento de chaves criptográficas e o controle do seu uso em uma ampla variedade de serviços da AWS e em seus aplicativos. O AWS KMS é um serviço seguro e resiliente que usa módulos de segurança de hardware validados ou em processo de validação pelo FIPS 140-2 para proteger suas chaves. O AWS KMS também é integrado ao AWS CloudTrail para fornecer logs contendo toda a utilização das chaves para ajudar a cumprir requisitos normativos e de conformidade.

O AWS KMS ajuda na centralização do gerenciamento e no armazenamento seguro de chaves. É possível gerar chaves no AWS KMS ou importá-las da sua própria infraestrutura de gerenciamento de chaves. Também é possível enviar dados diretamente para o AWS KMS para serem criptografados ou descriptografados. Outros serviços da AWS podem usar suas chaves em seu nome para proteger as chaves de criptografia de dados que eles usam para proteger seus dados.

Suas chaves nunca saem do AWS KMS e você está sempre no controle delas. É possível definir políticas de uso que determinam quais usuários podem usar as chaves e quais ações essas pessoas podem realizar. Todas as solicitações de uso dessas chaves são registradas no AWS CloudTrail para que você possa controlar quem usou qual chave, como e quando.

A criptografia do lado do servidor é a criptografia de dados em seu destino pelo aplicativo ou serviço que os recebe. O AWS Key Management Service (AWS KMS) é um serviço que combina hardware e software seguros e altamente disponíveis para fornecer um sistema de gerenciamento de chaves dimensionado para a nuvem. O Amazon S3 usa as Chaves Mestras do Cliente (CMKs) AWS KMS para criptografar seus objetos do Amazon S3. O AWS KMS criptografa apenas os dados do objeto. Todos os metadados do objeto não são criptografados.

O AWS KMS mantém e gerencia cada versão anterior da CMK para garantir que você possa descriptografar dados criptografados com versões anteriores.

Se você habilitar o AWS CloudTrail na sua conta, pode obter logs de chamadas de API feitas para ou pelo AWS KMS

É possível usar tags para categorizar e identificar CMKs e ajudar no monitoramento de custos da AWS. Ao adicionar tags a recursos da AWS, a AWS gera um relatório de alocação de custos para cada tag

Benefícios e recursos

Totalmente Gerenciado

Gerenciamento de Chaves centralizado

Integrado com serviços da AWS

Criptografia para todos os seus aplicativos

Auditoria integrada: O KMS é integrado ao AWS CloudTrail

Seguro e Confiável: O KMS usa armazenamento e arquitetura resilientes

Preço: Cada chave mestra do cliente (CMK) que você criar no AWS Key Management Service (KMS), custa 1 USD/mês até que seja excluída. O serviço oferece 20.000 solicitações gratuitas por mês. Ou seja, 1 USD pela chave e 20.000 solicitações de criptografia dos objetos e solicitações de decodificação para acessar os objetos

Você não será cobrado pelo seguinte:

Criação e armazenamento de CMKs gerenciados pela AWS. Essas chaves são criadas automaticamente em seu nome quando você tenta criptografar um recurso pela primeira vez em um serviço da AWS integrado ao AWS KMS. Você não pode gerenciar o ciclo de vida nem acessar permissões em chaves gerenciadas pela AWS.

CMKs administradas pelo cliente que você criou e que estão programadas para exclusão. Se você cancelar a exclusão durante o período de espera, serão cobradas taxas pela CMK como se ela nunca houvesse sido programada para exclusão.

Tipo de Chave

Simétrica: Uma única chave de criptografia usada para operações de criptografia

Assimétrica: Um par de chaves pública e privada que pode ser usada para criptografar/descriptografar ou assinar/verificar operações

Origem do Material de Chaves

A origem pode ser pelo próprio KMS ou externo

Regionalidade

Chave de Região Única: a chave nunca será replicada para outras regiões

Chave de Várias Regiões: permite que a chave seja replicada para outras regiões

Definir Permissões Administrativas da Chave

Escolha os **usuários e as funções** do IAM que podem administrar esta chave com a API do KMS. Talvez sejam necessárias permissões adicionais para que os usuários ou funções possam administrar essa chave a partir deste console. É opcional permitir que os administradores da chave, ou seja, os Usuários e as Funções, excluam a chave

Definir Permissões de Uso da Chave

Selecione os usuários e as funções do IAM que podem usar a CMK em operações de criptografia

➢ Pontos de Atenção

1. Você está trabalhando como arquiteto de soluções para um projeto governamental no qual está construindo um portal online para permitir que as pessoas paguem seus impostos e solicitem sua restituição online. Devido à confidencialidade dos dados, a política de segurança exige que o aplicativo hospedado no EC2 criptografe os dados antes de gravá-los no disco para armazenamento. Nesse cenário, qual serviço você usaria para atender a esse requisito? R: AWS KMS API

2. Você está liderando uma equipe de desenvolvimento de software que usa computação sem servidor com AWS Lambda para construir e executar aplicativos sem ter que configurar ou gerenciar servidores. Você tem uma função Lambda que se conecta a um MongoDB Atlas, que é uma plataforma de banco de dados como serviço (DBaaS) popular e também usa uma API de terceiros para buscar certos dados para seu aplicativo. Você instruiu um de seus desenvolvedores juniores a criar as variáveis de ambiente para o nome de host, nome de usuário e senha do banco de dados MongoDB, bem como as credenciais de API que serão usadas pela função Lambda para ambientes DEV, SIT, UAT e PROD. Considerando que a função Lambda está armazenando banco de dados confidenciais e credenciais de API, como você pode proteger essas informações para evitar que outros desenvolvedores em sua equipe, ou qualquer pessoa, vejam essas credenciais em texto simples? Selecione a melhor opção que forneça o máximo de segurança. R: Create a new KMS key and use it to enable encryption helpers that leverage on AWS Key Management Service to store and encrypt the sensitive information.

3. You are developing an application that uses the Amazon Kinesis Producer Library (KPL) to put data records to an encrypted Kinesis data stream. However, when your application runs, there is an unauthorized KMS master key permission error. How would you resolve the problem? R: In the KMS key policy, assign the permission to the application to access the key. Because the application would need to have permission to use the KMS key when putting records in the stream.

4. Sua recente análise de segurança revelou um grande aumento nas tentativas de login em sua conta da AWS. Para dados confidenciais armazenados no S3 habilitado para criptografia, os dados não foram criptografados e estão suscetíveis a fraude se forem roubados. Você recomendou o AWS Key Management Service como solução.

Qual das alternativas a seguir é verdadeira em relação à criptografia do lado do servidor do KMS? **R: Data is encrypted at rest with KMS.**

5. Você implementou o AWS Key Management Service para proteger seus dados em seus aplicativos e outros serviços AWS. Sua sede global fica na Virgínia do Norte (Leste dos Estados Unidos (Virgínia Norte), onde você criou suas chaves e forneceu as permissões apropriadas para usuários designados e funções específicas em sua organização. Enquanto os usuários norte-americanos não estão tendo problemas, alemão e japonês os usuários não conseguem fazer o KMS funcionar. Qual é a causa mais provável disso? **R: As chaves mestras KMS são específicas da região e os aplicativos estão acessando os terminais de API errados.**

6. Sua empresa usa KMS para gerenciar totalmente as chaves mestras e executar operações de criptografia e descriptografia em seus dados e aplicativos. Como um nível adicional de segurança, você agora recomenda que a AWS faça a rotação de suas chaves. O que aconteceria depois de habilitar esse recurso adicional? **R: Nothing needs to be done. KMS will manage all encrypt/decrypt actions using the appropriate keys.**

Amazon CloudHSM

O AWS CloudHSM é um Hardware Security Module (HSM – Módulo de segurança de hardware) baseado na nuvem que permite gerar e usar facilmente suas próprias chaves de criptografia na Nuvem AWS.

Com o CloudHSM, você pode gerenciar suas próprias chaves de criptografia usando HSMs validados pelo FIPS 140-2 nível 3. O CloudHSM oferece a flexibilidade de integrar-se aos seus aplicativos usando APIs padrão do setor, como bibliotecas Microsoft CryptoNG (CNG), PKCS#11 e Java Cryptography Extensions (JCE).

O CloudHSM está em conformidade com as normas do setor e permite exportar todas as chaves para a maioria dos outros HSMs disponíveis no mercado, dependendo das suas configurações.

Ele é um serviço gerenciado que automatiza para você tarefas administrativas demoradas, como provisionamento de hardware, aplicação de patches de software, alta disponibilidade e backups. O CloudHSM também permite que você ajuste a escala rapidamente ao adicionar e remover capacidade HSM sob demanda, sem custos antecipados.

Benefícios

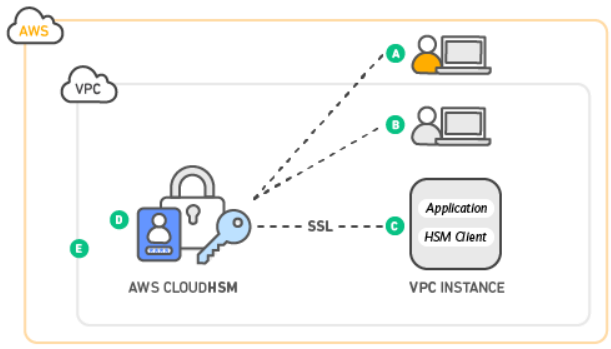
O AWS CloudHSM permite gerar e usar chaves de criptografia em um hardware validado pelo FIPS 140-2 nível 3. O CloudHSM protege suas chaves com acesso exclusivo e unilocatário a instâncias de HSMs invioláveis na sua própria Amazon Virtual Private Cloud (VPC).

O AWS CloudHSM disponibiliza acesso aos HSMs em um canal seguro para criar usuários e definir políticas de HSM. As chaves de criptografia geradas e usadas com o CloudHSM só podem ser acessadas pelos usuários de HSM que você especificar. A AWS não tem visibilidade ou acesso às suas chaves de criptografia.

O AWS CloudHSM automatiza tarefas administrativas demoradas, como provisionamento de hardware, aplicação de patches de software, alta disponibilidade e backups. É possível ajustar rapidamente a escala da capacidade do HSM ao adicionar e remover HSMs do cluster sob demanda. O AWS CloudHSM faz automaticamente as solicitações de balanceamento de carga e duplica com segurança as chaves armazenadas em qualquer HSM para todos os outros HSMs no cluster.

É possível configurar o AWS Key Management Service (KMS) para usar o cluster do AWS CloudHSM como um armazenamento de chaves personalizadas ao invés do armazenamento de chaves KMS padrão. Com um armazenamento de chaves personalizadas do KMS, você se beneficia da integração entre os serviços KMS e AWS que criptografam dados, mantendo o controle dos HSMs que protegem suas chaves mestras do KMS. O armazenamento de chaves personalizadas do KMS oferece o melhor dos dois mundos, combinando os HSMs de unilocatário sob seu controle com a facilidade de uso e a integração do AWS KMS.

Como Funciona



O AWS CloudHSM é executado na sua própria Amazon Virtual Private Cloud (VPC), o que permite usar de modo fácil os HSMs com aplicativos que rodam nas instâncias do Amazon EC2. Com o CloudHSM, é possível usar controles de segurança padrão da VPC para gerenciar o acesso aos HSMs. Os aplicativos conectam-se ao HSMs usando canais SSL mutuamente autenticados e estabelecidos pelo software cliente do HSM. Como os HSMs estão localizados nos datacenters da Amazon perto das instâncias do EC2, é possível reduzir a latência da rede entre os aplicativos e os HSMs, o que não é possível fazer da mesma maneira usando HSMs locais.

A: A AWS gerencia o dispositivo HSM, mas não tem acesso às chaves

B: Você controla e gerencia suas próprias chaves

C: A performance do aplicativo melhora (graças à grande proximidade com as cargas de trabalho da AWS)

D: O armazenamento seguro de chaves em hardware inviolável e disponível em várias zonas de disponibilidade (AZs)

E: Os HSMs estão na Virtual Private Cloud (VPC), isolados de outras redes da AWS.

A separação de responsabilidades e o controle de acesso baseado em funções são inerentes ao projeto do AWS CloudHSM. A AWS monitora a integridade e a disponibilidade de rede dos HSMs, mas não se envolve na criação e no gerenciamento do material de chaves armazenado dentro dos HSMs. Você controla os HSMs, bem como a geração e o uso das chaves de criptografia.

- **Pontos de Atenção**

There is a technical requirement by a financial firm that does online credit card processing to have a secure application environment on AWS. They are trying to decide on whether to use KMS or CloudHSM. Which of the following statements is right when it comes to CloudHSM and KMS? **R: You should consider using AWS CloudHSM over AWS KMS if you require your keys stored in dedicated, third-party validated hardware security modules under your exclusive control.**

Amazon Macie

Descubra e proteja seus dados confidenciais em escala

O Amazon Macie é um serviço de segurança e privacidade de dados totalmente gerenciado que usa machine learning e correspondência de padrões para descobrir e proteger seus dados confidenciais na AWS.

À medida que as organizações gerenciam volumes crescentes de dados, identificar e proteger seus dados confidenciais em escala pode se tornar cada vez mais complexo, caro e demorado. O Amazon Macie automatiza a descoberta de dados confidenciais em escala e reduz o custo da proteção de seus dados.

O Macie fornece automaticamente um inventário de buckets do Amazon S3, incluindo uma lista de buckets não criptografados, buckets acessíveis ao público e buckets compartilhados com as contas da AWS fora as definidas por você no AWS Organizations.

Em seguida, o Macie aplica técnicas de machine learning e de correspondência de padrões aos buckets selecionados para identificar e alertar sobre dados confidenciais, tais como informações de identificação pessoal (PII).

Os alertas ou descobertas do Macie podem ser pesquisados e filtrados no Console de Gerenciamento da AWS e enviados ao Amazon EventBridge, anteriormente chamado de Amazon CloudWatch Events para facilitar a integração com os sistemas de fluxo de trabalho ou de gerenciamento de eventos existentes ou para serem usados em combinação com os serviços da AWS, tais como o AWS Step Functions para executar ações de remediação automatizadas.

Isso pode ajudá-lo a cumprir regulamentos, como a Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA) e o Regulamento Geral de Privacidade de Dados (GDPR).

Você pode começar a usar o Amazon Macie aproveitando a avaliação gratuita de 30 dias para avaliação de bucket. O teste inclui 30 dias sem custo de uso do inventário do bucket do Amazon S3 e a avaliação do controle de segurança e acesso no nível do bucket.

Observe que a descoberta de dados confidenciais não está incluída na avaliação gratuita por 30 dias para avaliação de buckets.

Definição de Preço

Com o Amazon Macie, você é cobrado com base no número de buckets do Amazon S3 avaliados para controles de acesso e segurança em nível de bucket e na quantidade de dados processados para descoberta de dados confidenciais.

Número de buckets do Amazon S3 continuamente avaliados para controles de segurança e acesso — Quando você habilitar o Macie, o serviço reunirá detalhes em todos os buckets do S3, incluindo nomes de bucket, tamanho, contagem de objetos, tags de recursos, status de criptografia, controles de acesso e posicionamento de região. O Macie avaliará automaticamente e continuamente todos os seus buckets para segurança e controle de acesso, alertando-o sobre quaisquer buckets não criptografados, buckets acessíveis publicamente ou buckets compartilhados com uma conta da AWS fora da sua organização. Você será cobrado com base no número total de buckets na sua conta após a avaliação gratuita de 30 dias, e as cobranças são rateadas por dia.

Quantidade de dados processados para detecção de dados confidenciais — Depois de habilitar o serviço, você poderá configurar e enviar buckets para descoberta de dados confidenciais. Isso é feito selecionando os buckets que você gostaria de verificar, configurando um trabalho de descoberta de dados confidenciais ocasional ou periódica e enviando-o ao Macie. O Macie só cobra pelos bytes processados nos tipos de objeto com suporte que ele inspeciona. Como parte dos trabalhos de descoberta de dados sensíveis do Macie, você também incorrerá nas cobranças padrão do Amazon S3 para solicitações GET e LIST.

Formatos de arquivo e armazenamento com suporte no Amazon Macie

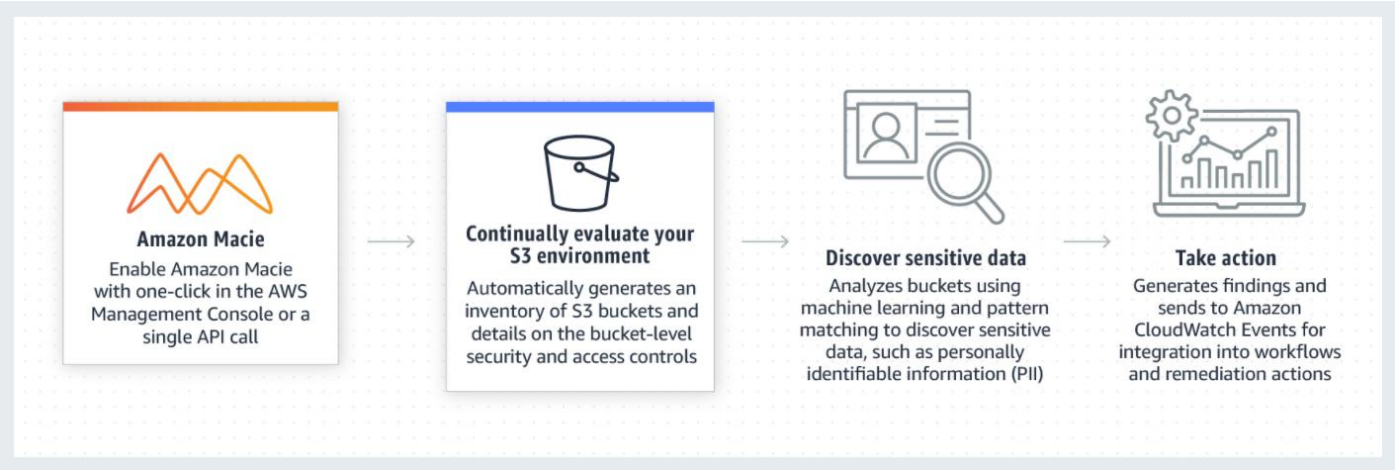
Quando o Amazon Macie analisa os dados, ele realiza uma inspeção profunda que considera o arquivo ou formato de armazenamento dos dados. O Macie pode analisar dados em muitos formatos diferentes, incluindo compactação

e formatos de arquivo comumente usados. Esse suporte se aplica ao uso de identificadores de dados gerenciados e identificadores de dados personalizados.

Quando o Macie analisa um arquivo compactado ou compactado, ele inspeciona o arquivo completo e o conteúdo do arquivo. Para inspecionar o conteúdo do arquivo, ele descompacta o arquivo e, em seguida, inspeciona cada arquivo extraído que usa um formato compatível. Macie pode fazer isso para até 1.000.000 de arquivos e até uma profundidade aninhada de 10 níveis.

A tabela a seguir lista e descreve os formatos de arquivo e armazenamento que o Macie pode analisar, organizados por tipo. Para cada tipo suportado, ele também lista as extensões de nome de arquivo aplicáveis.

File or storage type	Description	File name extensions
Big data	Apache Avro object containers and Apache Parquet files	.avro, .parquet
Compression or archive	GNU Zip compressed archives, TAR archives, and ZIP compressed archives	.gz, .gzip, .tar, .zip
Document	Adobe Portable Document Format files, Microsoft Excel workbooks, and Microsoft Word documents	.doc, .docx, .pdf, .xls, .xlsx
Text	Non-binary text files such as comma-separated values (CSV) files, Hypertext Markup Language (HTML) files, JavaScript Object Notation (JSON) files, JSON Lines files, plain-text documents, tab-separated values (TSV) files, and Extensible Markup Language (XML) files	.csv, .htm, .html, .json, .jsonl, .tsv, .txt, .xml, and others (depending on the type of non-binary text file)



AWS Secrets Manager

Alterne, gerencie e recupere facilmente credenciais de banco de dados, chaves de API e outros segredos durante seus ciclos de vida

O AWS Secrets Manager ajuda você a proteger os segredos necessários para acesso a aplicativos, serviços e recursos de TI. O serviço permite alternar, gerenciar e recuperar facilmente credenciais de banco de dados, chaves de APIs e outros segredos durante todo o seu ciclo de vida.

Os usuários e os aplicativos recuperam os segredos com uma chamada às APIs do Secrets Manager, o que elimina a necessidade de codificar informações confidenciais em texto simples. O Secrets Manager oferece alternância de segredos com integração incorporada para o Amazon RDS, Amazon Redshift e Amazon DocumentDB.

Além disso, o serviço pode ser estendido a outros tipos de segredos, incluindo chaves de API e tokens do OAuth. O Secrets Manager também permite controlar o acesso aos segredos usando permissões detalhadas e auditando a alternância de segredos de forma centralizada para recursos na Nuvem AWS, em serviços de terceiros ou no local.

Definição de Preço

O AWS Secrets Manager permite alternar, gerenciar e recuperar segredos durante todo o ciclo de vida, facilitando a manutenção de um ambiente seguro que atenda às suas necessidades de segurança e conformidade. Com o Secrets Manager, você paga pelo número de segredos armazenados e de chamadas de API efetuadas.

Links Úteis

https://docs.aws.amazon.com/secretsmanager/latest/userguide/aws-config-rules.html
https://docs.aws.amazon.com/config/latest/developerguide/secretsmanager-rotation-enabled-check.html

➢ Pontos de Atenção

1. Você planeja gerenciar chaves de API no AWS Secrets Manager. As chaves precisam ser giradas automaticamente para estar em conformidade com a política da empresa. No Secrets Manager, os aplicativos podem obter a versão mais recente das credenciais da API. Como você implementaria a rotação de chaves? R: Customize the Lambda function that performs the rotation of secrets in Secrets Manager.

2. Your organization starts to store RDS credentials in AWS Secrets Manager. To be compliant with security regulations, all secrets stored in the Secrets Manager should automatically rotate. If rotation is not enabled for a secret, your team should get an email notification. Which method is the most appropriate? R: Add the rule “secretsmanager-rotation-enabled-check” in AWS Config to check whether AWS Secrets Manager has enabled the secret rotation. Because the AWS Config rule “secretsmanager-rotation-enabled-check” checks whether AWS Secrets Manager secret has rotation enabled. Users need to add the rule in AWS Config and set up a notification.

AWS Shield

Proteção gerenciada contra DDoS

Um ataque de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

O AWS Shield é um serviço gerenciado de proteção contra DDoS (Negação de serviço distribuída) que protege os aplicativos executados na AWS. O AWS Shield oferece de detecção e mitigações em linha automáticas e sempre ativas que minimizam o tempo de inatividade e a latência dos aplicativos, fornecendo proteção contra DDoS sem necessidade de envolver o AWS Support**. O AWS Shield tem dois níveis, Standard e Advanced.**

Todos os clientes da AWS se beneficiam gratuitamente com as proteções automáticas do AWS Shield Standard. O AWS Shield Standard protege contra os ataques de DDoS mais comuns, que ocorrem com frequência nas camadas de rede e transporte e visam sites ou aplicativos web. Ao usar o AWS Shield Standard com o Amazon CloudFront e o Amazon Route 53, você recebe uma proteção abrangente de disponibilidade contra todos os ataques conhecidos de infraestrutura (camadas 3 e 4).

Para obter níveis mais altos de proteção contra ataques direcionados a seus aplicativos executados em recursos do Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator e Amazon Route 53, você pode inscrever-se no AWS Shield Advanced. Além das proteções nas camadas de rede e transporte fornecidas com a versão Standard, o AWS Shield Advanced fornece detecção e mitigação adicionais contra ataques grandes e sofisticados de DDoS, visibilidade praticamente em tempo real aos ataques e integração ao AWS WAF, um firewall para aplicativo web. Além disso, o AWS Shield Advanced oferece acesso 24x7 à AWS DDoS Response Team (DRT – Equipe de resposta a DDoS) e proteção contra picos relacionados a DDoS em suas cobranças do Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator e Amazon Route 53.

O AWS Shield Advanced está disponível globalmente em todos os pontos de presença do Amazon CloudFront, AWS Global Accelerator e Amazon Route 53. Você pode proteger seus aplicativos web hospedados em qualquer lugar do mundo implantando o Amazon CloudFront acima de seu aplicativo. Os servidores de origem podem ser o Amazon S3, o Amazon Elastic Compute Cloud (EC2), o Elastic Load Balancing (ELB) ou um servidor personalizado fora da AWS. Também é possível habilitar o AWS Shield Advanced diretamente em um IP elástico ou em um Elastic Load Balancing (ELB) nestas regiões da AWS: Norte da Virgínia, Ohio, Oregon, Norte da Califórnia, Montreal, São Paulo, Irlanda, Frankfurt, Londres, Paris, Estocolmo, Singapura, Tóquio, Sydney, Seul e Mumbai.

AWS Shield Standard

Proteção de DDoS de limite estático para serviços AWS subjacentes

O AWS Shield Standard oferece um monitoramento de fluxo de rede sempre ativo que inspeciona o tráfego de entrada da AWS e aplica uma combinação de assinaturas de tráfego, algoritmos de anomalias e outras técnicas de análise para detectar tráfego mal-intencionado em tempo real. O Shield Standard define limites estáticos para cada tipo de recurso da AWS, mas não fornece qualquer proteção para aplicações do cliente da AWS.

Mitigação de ataques em linha

As técnicas de mitigação automática são criadas no AWS Shield Standard, oferecendo a proteção dos serviços da AWS contra ataques comuns e frequentes à infraestrutura. Mitigações automáticas são aplicadas em linha para proteger os serviços da AWS, sem afetar a latência. O AWS Shield Standard usa técnicas, como filtragem determinística de pacotes e modelagem de tráfego com base em prioridade para mitigar automaticamente os ataques na camada de rede básicos.

AWS Shield Advanced

Detecção personalizada com base em padrões de tráfego da aplicação

O AWS Shield Advanced fornece detecção personalizada com base em padrões de tráfego para seus recursos protegidos de endereço IP elástico, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator ou Amazon Route 53. Usando técnicas adicionais de monitoramento específicas de regiões e recursos, o AWS Shield Advanced detecta e alerta sobre ataques de DDoS menores. O AWS Shield Advanced também detecta ataques na camada de aplicações, como floods de HTTP ou floods de consultas de DNS, ao definir uma linha de base de tráfego para seus recursos e identificar anomalias.

Detecção com base na integridade

O AWS Shield Advanced usa a integridade de suas aplicações para aprimorar a responsividade e a precisão na detecção e mitigação de ataques. Agora você pode definir uma verificação de integridade no Amazon Route 53 e associá-la a um recurso que seja protegido pelo Shield Advanced por meio do console ou da API. Isso permite que o Shield Advanced detecte ataques que afetam a integridade de sua aplicação rapidamente e com limites menores de tráfego, melhorando a resiliência da sua aplicação contra DDoS e prevenindo a notificação de falsos positivos. O status de integridade dos recursos também estará disponível para a equipe de resposta a DDoS para que eles possam priorizar adequadamente a resposta a aplicações prejudiciais primeiro. É possível aplicar a detecção baseada em integridade a todos os tipos de recursos compatíveis com o Shield Advanced: Elastic IP, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator ou Amazon Route 53.

Mitigação avançada de ataques

O AWS Shield Advanced oferece mitigações automáticas mais sofisticadas para ataques direcionados a suas aplicações executadas em recursos protegidos do Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator e Amazon Route 53. O AWS Shield Advanced usa técnicas de roteamento avançadas para implantar automaticamente capacidade adicional de mitigação e proteger contra ataques de DDoS de grande porte. Para clientes com suporte Business ou Enterprise, o AWS DDoS Response Team (DRT) também aplica mitigações manuais em caso de ataques DDoS mais complexos e sofisticados que podem ser exclusivos para sua aplicação. Para ataques à camada de aplicação, você pode usar o AWS WAF sem custo adicional para os recursos protegidos do AWS Shield Advanced, para configurar regras proativas, como bloqueio com base em taxa para bloquear automaticamente as solicitações da Web de ataque de endereços IP de origem, ou responder imediatamente a incidentes à medida que eles ocorrerem. Você também pode interagir diretamente com o DRT para implementar regras do AWS WAF personalizadas em seu nome como resposta a um ataque DDoS à camada da aplicação. O DRT diagnosticará o ataque e, com sua permissão, poderá aplicar atenuações em seu nome, reduzindo a quantidade de tempo que suas aplicações podem ser afetadas por um ataque DDoS em andamento.

Resposta proativa do evento

Agora, o AWS Shield Advanced oferece o envolvimento proativo do DDoS Response Team (DRT) quando um evento DDoS é detectado. Quando você ativar o envolvimento proativo, o DRT entrará em contato diretamente com você se uma verificação de integridade do Amazon Route 53 associada ao seu recurso protegido tornar-se insatisfatória durante um evento DDoS. Isso permite que você interaja com especialistas mais rapidamente quando a disponibilidade da sua aplicação puder ser afetada por um ataque suspeito. Você pode receber envolvimento proativo para eventos de camada de rede e camada de transporte em endereços IP elásticos e aceleradores do Global Accelerator e para ataques de camada da aplicação em distribuições do CloudFront e em Application Load Balancers.

➢ Pontos de Atenção

You have identified a series of DDoS attacks while monitoring your VPC. As the Solutions Architect, you are responsible in fortifying your current cloud infrastructure to protect the data of your clients. Which of the following is the most suitable solution to mitigate these kinds of attacks? R: Use AWS Shield to detect and mitigate DDoS attacks.

AWS Single Sign-On

Gerencie o acesso de SSO (logon único) de forma centralizada para várias contas e aplicativos de negócios da AWS.

O logon único é um esquema de autenticação que permite ao usuário fazer logon com um único ID e senha em qualquer um dos vários sistemas de software relacionados, mas independentes.

O AWS Single Sign-On é um serviço de logon único (SSO) baseado em nuvem que facilita o gerenciamento centralizado do acesso SSO a todas as suas contas da AWS e aplicativos em nuvem. Especificamente, ele ajuda a gerenciar o acesso SSO e as permissões do usuário em todas as suas contas AWS no AWS Organizations. O AWS SSO também ajuda a gerenciar o acesso e as permissões para aplicativos de software como serviço (SaaS) de terceiros comumente usados, aplicativos integrados com SSO da AWS, bem como aplicativos personalizados que oferecem suporte a Security Assertion Markup Language (SAML) 2.0. O AWS SSO inclui um portal de usuário onde seus usuários finais podem encontrar e acessar todas as suas contas AWS atribuídas, aplicativos em nuvem e aplicativos personalizados em um só lugar.

Integração com AWS Organizations

O AWS SSO está profundamente integrado às organizações AWS e às operações de API da AWS, ao contrário de outras soluções SSO nativas em nuvem. O AWS SSO se integra nativamente ao AWS Organizations e enumera todas as suas contas da AWS. Se você organizou suas contas em unidades organizacionais (OUs), você as verá exibidas dessa forma no console de SSO da AWS. Dessa forma, você pode descobrir rapidamente suas contas AWS, implantar conjuntos comuns de permissões e gerenciar o acesso de um local central.

Acesso SSO a suas contas AWS e aplicativos em nuvem

O AWS SSO simplifica o gerenciamento do SSO em todas as suas contas AWS, aplicativos em nuvem, aplicativos integrados ao AWS SSO e aplicativos baseados em SAML 2.0 personalizados, sem scripts personalizados ou soluções SSO de terceiros. Use o console AWS SSO para atribuir rapidamente quais usuários devem ter acesso com um clique apenas aos aplicativos que você autorizou para seu portal de usuário final personalizado.

Crie e gerencie usuários e grupos no AWS SSO

Quando você habilita o serviço pela primeira vez, criamos um armazenamento padrão para você no AWS SSO. Você pode usar esta loja para gerenciar seus usuários e grupos diretamente no console. Ou, se preferir, você pode se conectar a um diretório AWS Managed Microsoft AD existente e gerenciar seus usuários com ferramentas de gerenciamento padrão do Active Directory fornecidas no Windows Server. Você também pode provisionar usuários e grupos de um provedor de identidade externo no AWS SSO e gerenciar permissões de acesso no console AWS SSO. Se você optar por gerenciar seus usuários no AWS SSO, poderá criar usuários rapidamente e, em seguida, organizá-los facilmente em grupos, tudo dentro do console.

Potencialize suas identidades corporativas existentes

O AWS SSO é integrado ao Microsoft AD por meio do AWS Directory Service. Isso significa que seus funcionários podem entrar no portal do usuário SSO da AWS usando suas credenciais corporativas do Active Directory. Para conceder aos usuários do Active Directory acesso a contas e aplicativos, basta adicioná-los aos grupos apropriados do Active Directory. Por exemplo, você pode conceder ao grupo DevOps acesso SSO às suas contas de produção da AWS. Os usuários adicionados ao grupo DevOps recebem acesso SSO a essas contas da AWS automaticamente. Essa automação facilita a integração de novos usuários e fornece aos usuários existentes acesso a novas contas e aplicativos rapidamente.

Compatível com aplicativos em nuvem comumente usados

O SSO da AWS oferece suporte a aplicativos em nuvem comumente usados, como Salesforce, Box e Office 365. Isso reduz o tempo necessário para configurar esses aplicativos para SSO, fornecendo instruções de integração de aplicativos. Essas instruções atuam como guarda-corpos para ajudar os administradores a definir e solucionar problemas dessas configurações de SSO. Isso elimina a necessidade de os administradores aprenderem as nuances de configuração de cada aplicativo em nuvem.

Fácil de configurar e monitorar o uso

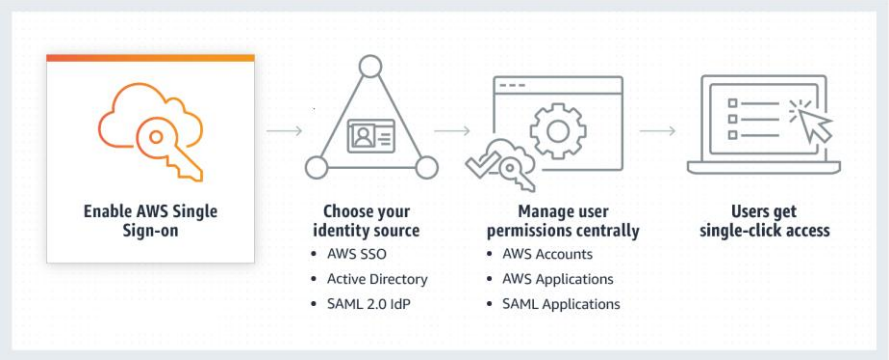
Com o AWS SSO, você pode habilitar um serviço SSO altamente disponível com apenas alguns cliques. Não há infraestrutura adicional para implantar ou conta AWS para configurar. O AWS SSO é uma infraestrutura altamente disponível e totalmente segura que se adapta às suas necessidades e não requer software ou hardware para gerenciar. O AWS SSO registra todas as atividades de login no AWS CloudTrail, dando a você a visibilidade para monitorar e auditar a atividade SSO em um só lugar.

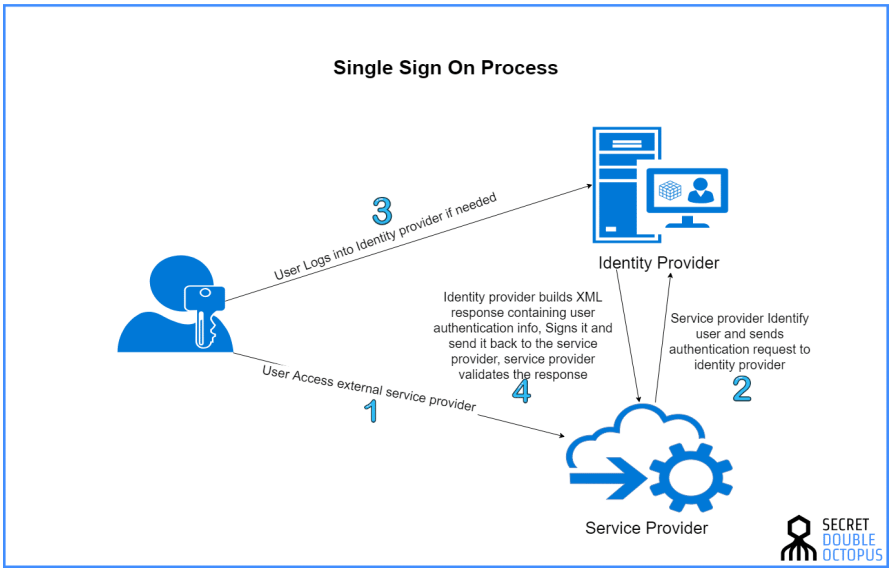
Coexiste com usuários, funções e políticas existentes do IAM

A ativação do SSO da AWS, incluindo a ativação de Organizações da AWS, não tem impacto sobre os usuários, funções ou políticas que você já está gerenciando no IAM. Você pode continuar a usar seus processos e ferramentas de gerenciamento de acesso existentes à medida que sua organização adota o AWS SSO.

Gerenciamento de identidade sem custo

Você pode adicionar qualquer conta AWS gerenciada usando AWS Organizations para AWS SSO. Tanto o AWS SSO quanto o AWS Organizations estão disponíveis sem custo adicional.





➢ Pontos de Atenção

1. Você está trabalhando como arquiteto da AWS para um cliente corporativo. Os usuários acessam buckets do Amazon S3 para salvar todos os documentos relacionados ao projeto e usam aplicativos de negócios como o Office 365 para atividades de trabalho diárias. Esses aplicativos precisam estar acessíveis de qualquer dispositivo por um número limitado de horas durante o dia. Eles estão usando o AWS SSO para gerenciar e controlar o acesso aos recursos da AWS de forma centralizada. Os usuários estão reclamando que estão obtendo logout do console e precisam fazer o login novamente a cada hora. Você precisa se certificar de que a sessão do usuário é ideal com base na conclusão da atividade. Qual das opções a seguir pode ser definida para atender a esse requisito? R: Create a custom Permission Set with session duration as 6 hours.

Permission sets can control the time duration for user login to the AWS Console by setting session duration. The Default Session duration is 1 hour, while the maximum can be set to 12 hours. Post this session duration. The user is automatically logout.

AWS Single Sign-On (SSO) enables you to customize the session duration to AWS accounts ranging from **1 hour up to 12 hours**. You can configure session duration for each permission set so that you can optimize how long your users can access the AWS Management Console and AWS CLI for your AWS accounts. For example, when your users need to run long-running operations, you can increase the session duration to complete the operation using a single session.

AWS WAF (Web Application Firewall)

O AWS WAF é um firewall de aplicações Web que ajuda a proteger suas aplicações Web ou APIs contra bots e exploits comuns na Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos em excesso.

O AWS WAF oferece controle sobre como o tráfego atinge suas aplicações, permitindo que você crie regras de segurança que controlam o tráfego de bots e bloqueiam padrões de ataque comuns, como injeção de SQL ou cross-site scripting.

Injeção de SQL (do inglês SQL Injection) é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados através de comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta (SQL query) através da entradas de dados de uma aplicação, como formulários ou URL de uma aplicação (Wikipedia)

Cross-site scripting (XSS) é um tipo de vulnerabilidade do sistema de segurança de um computador, encontrado normalmente em aplicações web que ativam ataques maliciosos ao injetarem client-side script dentro das páginas web vistas por outros usuários. Um script de exploração de vulnerabilidade cross-site pode ser usado pelos atacantes para escapar aos controles de acesso que usam a política de mesma origem.

A linguagem de cliente ou client-side scripting, é uma linguagem que é executada no lado cliente, ou seja, no computador do próprio usuário, e por isso é usada nas situações em que a linguagem server-side não tem alcance.

Você também pode personalizar regras que filtram padrões de tráfego específicos. Você pode começar rapidamente usando regras gerenciadas para o AWS WAF, um conjunto pré-configurado de regras gerenciadas pela AWS ou por vendedores do AWS Marketplace para resolver problemas como os dez principais riscos de segurança e bots automatizados do OWASP que consomem recursos em excesso, distorcem métricas ou podem causar um tempo de inatividade.

OWASP - Open Web Application Security Project é uma comunidade aberta dedicada a permitir que as organizações desenvolvam, adquiram e mantenham aplicações e APIs confiáveis.

Essas regras são atualizadas regularmente conforme surgem novos problemas. O AWS WAF inclui uma API multifuncional que você pode usar para automatizar a criação, a implantação e a manutenção de regras de segurança.

Você pode implantar o AWS WAF no Amazon CloudFront como parte de uma solução de CDN, no Application Load Balancer que faz frente aos servidores Web ou de origem executados no EC2, no Amazon API Gateway para suas APIs REST ou no AWS AppSync para suas APIs GraphQL.

Regras

A AWS já possui diversas regras pré-definidas para utilizar. Uma regra define padrões de ataque a serem procurados em solicitações da web e a ação a ser executada quando uma solicitação corresponde aos padrões. Os grupos de regras são coleções reutilizáveis de regras. Você pode usar grupos de regras gerenciadas oferecidos por vendedores AWS e AWS Marketplace. Você também pode escrever suas próprias regras e usar seus próprios grupos de regras. Se uma solicitação corresponder a uma regra, execute a ação correspondente

Alguns exemplos de ataques que as regras atendem, bloqueando (Dany) / permitindo (Allow) a continuação da requisição: XSS, IP, Geolocalização, Query String, SQL Code

Por exemplo: um solicitante específico está realizando um ataque DoS de 1000 requisições/segundo, o WAF que está vinculado a um Load Balancer, começa a filtrar a requisição para uma lista de IPs restritos, onde toda a vez que houver uma requisição vinda daquele IP, a requisição será bloqueada, retornando um Dany para o solicitante

IP Set

Um conjunto de IP é uma coleção de endereços IP e intervalos de endereços IP que você usa em uma declaração de regra. Para usar um conjunto de IP em uma ACL da web ou grupo de regras, primeiro você cria um conjunto de IP com as especificações de seu endereço IP. Em seguida, você faz referência ao conjunto ao adicionar a instrução de regra de conjunto de IP a uma ACL da web ou grupo de regras.

Conjuntos de IP e conjuntos de padrão de Regex

Quando você faz alterações em ACLs da web ou componentes de ACL da web, como regras e grupos de regras, o AWS WAF propaga as mudanças em todos os lugares em que a ACL da web e seus componentes são armazenados e usados. Suas alterações são aplicadas em segundos, mas pode haver um breve período de inconsistência quando as alterações chegam em alguns lugares e não em outros. Assim, por exemplo, se você adicionar um endereço IP a um conjunto de IPs que é referenciado por uma regra de bloqueio em uma ACL da web, o novo endereço pode ser bloqueado brevemente em uma área enquanto ainda é permitido em outra. Essa inconsistência temporária pode ocorrer quando você associa pela primeira vez uma ACL da web a um recurso da AWS e quando altera uma ACL da web que já está associada a um recurso. Geralmente, quaisquer inconsistências desse tipo duram apenas alguns segundos.

Definição de Preço

Com o AWS WAF, você paga apenas pelo que usar e o preço é baseado em quantas regras você implanta e quantas solicitações da Web sua aplicação recebe

A cobrança do AWS WAF é feita com base no número de listas de controle de acesso da web (ACLs da web) criadas, no número de regras adicionadas para cada ACL da web e no número de solicitações da web recebidas. Não há compromissos antecipados. As cobranças do AWS WAF são adicionadas às definições de preço do Amazon **CloudFront**, **Application Load Balancer** (ALB), **Amazon API Gateway** e/ou **AWS AppSync**

Você será cobrado por cada ACL da Web que criar e cada regra criada por ACL da Web. Além disso, você será cobrado pelo número de solicitações da web processadas pela ACL da Web.

Tipo de recurso	Preço
ACL da web	5,00 USD por mês (hora rateada)
Regra	1,00 USD por mês (hora rateada)
Solicitação	0,60 USD por 1 milhão de solicitações

Links Úteis

https://www.youtube.com/watch?v=z6CV52iZtrM

https://wiki.owasp.org/images/0/06/OWASP_Top_10-2017-pt_pt.pdf

➢ Pontos de Atenção

You have a PHP application deployed in an Auto Scaling group. In production, you want to use AWS WAF to block requests associated with exploiting vulnerabilities specific to the PHP use, including injection of unsafe PHP functions. Which method is appropriate? R: Add the AWS managed PHP application rule in the web ACL of AWS WAF

AWS Resource Access Manager (RAM)

Simple, secure service to share AWS resources

AWS Resource Access Manager (RAM) helps you securely share your resources across AWS accounts, within your organization or organizational units (OUs) in AWS Organizations, and with IAM roles and IAM users for supported resource types. You can use AWS RAM to share transit gateways, subnets, AWS License Manager license configurations, Amazon Route 53 Resolver rules, and more resource types.

Many organizations use multiple accounts to create administrative or billing isolation, and to limit the impact of errors. With AWS RAM, you don't need to create duplicate resources in multiple AWS accounts. This reduces the operational overhead of managing resources in every account that you own. Instead, in your multi-account environment, you can create a resource once, and use AWS RAM to share that resource across accounts by creating a resource share. When you create a resource share, you select the resources to share, choose an AWS RAM managed permission per resource type, and specify whom you want to have access to the resources. AWS RAM is available to you at no additional charge.

RAM leverages existing policies and permissions set in AWS Identity and Access Management (IAM) to govern the consumption of shared resources. RAM also provides comprehensive visibility into shared resources to set alarms and visualize logs through integration with Amazon CloudWatch and AWS CloudTrail.

Sharing resources such as AWS License Manager configurations across accounts allows you to leverage licenses in multiple parts of your company to increase utilization and optimize costs.

Links Úteis

https://aws.amazon.com/pt/blogs/aws/new-aws-resource-access-manager-cross-account-resource-sharing/

- **Pontos de Atenção**

You work in a large organization. Your team creates AWS resources such as Amazon EC2 dedicated hosts and reserved capacities that need to be shared by other AWS accounts. You need an AWS service to centrally manage these resources so that you can easily specify which accounts or Organizations can access the resources. Which AWS service would you choose to meet this requirement? **R: Resource Access Manager**